

REMARKS

Claims 1-26 remain in the present application. Applicants respectfully request further examination and reconsideration of the rejections based on the arguments set forth below.

Claim Rejections – 35 U.S.C. §103

Claims 1-3, 5-7, 9-11, 14-15, 18-21 and 26

Claims 1-3, 5-7, 9-11, 14-15, 18-21 and 26 are rejected under 35 U.S.C. §103(a) as being unpatentable over United States Patent Number 5,563,950 to Easter et al. (hereafter referred to as “Easter”) in view of United States Patent Number 4,634,807 to Chorley et al. (hereafter referred to as “Chorley”).

Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claims 1-3, 5-7, 9-11, 14-15, 18-21 and 26 are not rendered obvious by Easter in view of Chorley for the following reasons.

Applicants respectfully direct the Examiner to independent Claim 1 that recites a processor with secure cryptographic capabilities comprising (emphasis added):

a digital secret comprising a secret key used in a key-based cryptographic process, wherein said digital secret is stored only within said processor, and wherein said digital secret is operable to be used exclusively by said processor for both encryption and decryption;
a cryptography engine for performing said key-based cryptographic process internally within said processor, said cryptography engine operable to access said digital secret; and
internal memory coupled to said cryptography engine for supporting said key-based cryptographic process.

Independent Claims 10 and 21 recite limitations similar to independent Claim 1. Claims 2-3, 5-7, 9, 11, 14-15, 18-20 and 26 depend from their respective independent Claims and recite further limitations to the claimed invention.

Applicants respectfully submit that Easter fails to teach or suggest the limitations of “wherein said digital secret is stored only within said processor” as recited in independent Claim 1. As recited and described in the present application, a digital secret includes a secret key used in a key-based cryptographic process. The digital secret is stored only within the processor.

In contrast to the claimed embodiments, Applicants understand Easter to teach storing a key outside of a processor. For example, Easter teaches that keys are stored within key array 25, where key array 25 is located within integrated circuit 53 (Figure 5; col. 8, line 18). As shown in Figure 5 of Easter, IC 53 is separate from CPU 13. Additionally, as acknowledged on page 3 of the rejection, IC 53 is not a processor as claimed. Accordingly, assuming *arguendo* that CPU 13 as taught by Easter is analogous to a processor as claimed, and further assuming *arguendo* that a key within key array 25 as taught by Easter is analogous to a digital secret as claimed, Easter teaches away from the claimed embodiments by teaching storing a key *outside* a processor instead of *within* a processor as claimed.

Moreover, Easter teaches that the keys stored within key array 25 are *public* keys (col. 4, lines 63-65; col. 8, lines 20-22). Applicants respectfully

submit that public keys as taught by Easter are not digital secrets, or secret keys, as claimed. Accordingly, Applicants reiterate that Easter teaches away from the claimed embodiments.

Additionally, Applicants respectfully submits that Chorley, either alone or in combination with Easter, also fails to teach or suggest the limitations of “wherein said digital secret is stored only within said processor” as recited in independent Claim 1. In contrast to the claimed embodiments, Applicants understand Chorley to teach decrypting and running software within a secure processor using keys (col. 1, lines 34-39). However, Applicants fail to find any teaching or suggestion in Chorley that the keys used to decrypt the software are *only* stored within the processor as claimed. Accordingly, Applicants reiterate that Chorley also fails to teach or suggest the limitations of “wherein said digital secret is stored only within said processor” as recited in independent Claim 1.

Applicants respectfully submit that Easter fails to teach or suggest the limitations of “wherein said digital secret and said internal memory are fully integrated with said cryptography engine to facilitate communication without use of a bus” as recited in Claim 19, and similarly recited in Claim 26. As recited and described in the present application, the digital secret and the internal memory are fully integrated with the cryptography engine to facilitate communication *without use of a bus*. For example, in one embodiment, the digital secret, internal memory and cryptography engine may be hardwired together to facilitate

communication without use of a bus (Figure 4; line 25 of page 18 to line 6 of page 19).

In contrast to the claimed embodiments, Applicants understand Easter to teach key array 25 coupled to DES engine 21 by bus 37 (Figure 5). Assuming *arguendo* that key array 25 is analogous to an internal memory as claimed, also assuming *arguendo* that a key of key array 25 is analogous to a digital secret as claimed, and further assuming *arguendo* that DES engine 21 is analogous to a cryptography engine as claimed, Applicants respectfully submit that Easter teaches away from the claimed embodiments by teaching that the components communicate via bus 37 instead of *without the use of a bus* as claimed. Additionally, Applicants respectfully submit that Easter further teaches away from the claimed embodiments by teaching that the keys within key array 25 are public keys as discussed above instead of digital secrets as claimed.

Additionally, Applicants respectfully submit that Chorley, either alone or in combination with Easter, fails to cure the deficiencies of Easter discussed above. More specifically, Applicants respectfully submit that Chorley, either alone or in combination with Easter, also fails to teach or suggest the limitations of “wherein said digital secret and said internal memory are fully integrated with said cryptography engine to facilitate communication without use of a bus” as recited in Claim 19, and similarly recited in Claim 26.

Furthermore, Applicants respectfully submit that one of ordinary skill in the art would not be motivated to implement Easter's IC 53 within Chorley's processor. For example, Easter teaches away from such a combination by teaching components of IC 53 *separate from* CPU 13 (Figure 2; Figure 5). Further, Chorley teaches that the security of the processor is poor and that "[a]n intruder could, for example, load software into the secure processor, the software being designed to disclose the keys or other sensitive information stored within it" (col. 1, lines 47-50). Accordingly, Chorley teaches that a combination of Easter and Chorley in the claimed fashion would decrease the security of information and reveal keys and other sensitive information, and therefore, Applicants reiterate that one of ordinary skill in the art would not be motivated to combine Easter and Chorley in the claimed fashion.

For these reasons, Applicants respectfully submit that independent Claim 1 is not rendered obvious by Easter in view of Chorley, thereby overcoming the 35 U.S.C. §103(a) rejection of record. Since independent Claims 10 and 21 recite limitations similar to those discussed above with respect to independent Claim 1, independent Claims 10 and 21 also overcomes the 35 U.S.C. §103(a) rejection of record. Since dependent Claims 2-3, 5-7, 9, 11, 14-15, 18-20 and 26 recite further limitations to the invention claimed in their respective independent Claims, Claims 2-3, 5-7, 9, 11, 14-15, 18-20 and 26 are also not rendered obvious by Easter in view of Chorley. Therefore, Claims 1-3, 5-7, 9-11, 14-15, 18-21 and 26 are allowable.

Claim 4

Claim 4 is rejected under 35 U.S.C. §103(a) as being unpatentable over Easter in view of Chorley, further in view of United States Patent Number 6,598,165 to Galasso (hereafter referred to as “Galasso”), and further in view of United States Patent Application Publication Number 2004/0243823 (hereafter referred to as “Moyer”). Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claim 4 are not rendered obvious by Easter in view of Chorley in view of Galasso and further in view of Moyer for the following reasons.

Applicants respectfully submit that Galasso and/or Moyer, either alone or in combination with the cited Easter/Chorley combination, fail to cure the deficiencies of Easter and Chorley discussed above with respect to independent Claim 1. Specifically, Galasso and/or Moyer fail to teach or suggest the limitations of “wherein said digital secret is stored only within said processor” as recited in independent Claim 1. Consequently, since Claims 4 recites further limitations to the invention claimed in independent Claim 1, Claim 4 is not rendered obvious by Easter in view of Chorley in view of Galasso and further in view of Moyer. Thus, Claim 4 overcomes the 35 U.S.C. §103(a) rejection of record.

Claims 8, 13 and 22

Claims 8, 13 and 22 are rejected under 35 U.S.C. §103(a) as being unpatentable over Easter in view of Chorley and further in view of United States

Patent Application Publication Number 2004/0098591 by Fahrny (hereafter referred to as "Fahrny"). Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claims 8, 13 and 22 are not rendered obvious by Easter in view of Chorley in view of Fahrny for the following reasons.

Applicants respectfully submit that Fahrny, either alone or in combination with the cited Easter/Chorley combination, fails to cure the deficiencies of Easter and Chorley discussed above with respect to independent Claims 1, 10 and 21. Specifically, Fahrny fails to teach or suggest the limitations of "wherein said digital secret is stored only within said processor" as recited in independent Claim 1, and similarly recited in independent Claims 10 and 21. Consequently, since Claims 8, 13 and 22 recite further limitations to the invention claimed in their respective independent Claims, Claims 8, 13 and 22 are not rendered obvious by Easter in view of Chorley in view of Fahrny. Thus, Claims 8, 13 and 22 overcome the 35 U.S.C. §103(a) rejection of record.

Claim 12

Claim 12 is rejected under 35 U.S.C. §103(a) as being unpatentable over Easter in view of Chorley in view of United States Patent Number 6,031,992 to Cmelik et al. (hereafter referred to as "Cmelik"). Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claim 12 is not rendered obvious by Easter in view of Chorley in view of Cmelik for the following reasons.

Applicants respectfully submit that Cmelik, either alone or in combination with the cited Easter/Chorley combination, fails to cure the deficiencies of Easter and Chorley discussed above with respect to independent Claim 10. Specifically, Cmelik fails to teach or suggest the limitations of “wherein said digital secret is stored only within said processor” as recited in independent Claim 1, and similarly recited in independent Claim 10. Consequently, since Claim 12 recites further limitations to the invention claimed in independent Claim 10, Claim 12 is not rendered obvious by Easter in view of Chorley and further in view of Cmelik. Thus, Claim 12 overcomes the 35 U.S.C. §103(a) rejection of record.

Claims 16-17

Claims 16-17 are rejected under 35 U.S.C. §103(a) as being unpatentable over Easter in view of Chorley and further in view of United States Patent Application Publication Number 2004/0025036 by Balard et al. (hereafter referred to as “Balard”). Applicants have reviewed the cited references and respectfully submit that the embodiments of the present invention as recited in Claims 16-17 are not rendered obvious by Okada in view of Balard for the following reasons.

Applicants respectfully submit that Balard, either alone or in combination with the cited Easter/Chorley combination, fails to cure the deficiencies of Easter and Chorley discussed above with respect to independent Claim 10. Specifically, Balard fails to teach or suggest the limitations of “wherein said digital secret is stored only within said processor” as recited in independent Claim 1, and

similarly recited in independent Claim 10. Consequently, since Claims 16-17 recite further limitations to the invention claimed in independent Claim 10, Claims 16-17 are not rendered obvious by Easter in view of Chorley and further in view of Balard. Thus, Claims 16-17 overcome the 35 U.S.C. §103(a) rejections of record.

Claims 23-24 and 26

Claims 23-24 and 26 are rejected under 35 U.S.C. §103(a) as being unpatentable over Easter in view of Chorley and further in view of Moyer. Applicants have reviewed the cited reference and respectfully submit that the embodiments of the present invention as recited in Claims 23-24 and 26 are not rendered obvious by Easter in view of Chorley and further in view of Moyer for the following reasons.

Applicants respectfully submit that Moyer, either alone or in combination with the cited Easter/Chorley combination, fails to cure the deficiencies of Easter and Chorley discussed above with respect to independent Claim 21. Specifically, Balard fails to teach or suggest the limitations of “wherein said digital secret is stored only within said processor” as recited in independent Claim 1, and similarly recited in independent Claim 21. Consequently, since Claims 23-24 and 26 recite further limitations to the invention claimed in independent Claim 21, Claims 23-24 and 26 are not rendered obvious by Easter in view of Chorley and further in view of Moyer. Thus, Claims 23-24 and 26 overcome the 35 U.S.C. §103(a) rejection of record.

CONCLUSION

Applicant respectfully submits that Claims 1-26 are in condition for allowance and Applicants earnestly solicit such action from the Examiner.

The Examiner is urged to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present application.

Please charge any additional fees or apply any credits to our PTO deposit account number: 50-4160.

Respectfully submitted,

MURABITO, HAO & BARNES LLP

Dated: 3 / 26 / 2008

/BMF/

Bryan M. Failing
Registration No. 57,974

Two North Market Street
Third Floor
San Jose, CA 95113
(408) 938-9060